PATENT

Atty Docket No.: 200207237-1
App. Ser. No.: 10/733,434

REMARKS

Favorable reconsideration of this application is respectfully requested in view of the following remarks. Claims 1-28 and 30-36 are pending in the present application of which claims 1, 11, 17, 19, 26, 28 and 36 are independent. Claim 29 is canceled herein and combined with independent claim 28.

Claims 1-36 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1-36 were rejected under 35 U.S.C. §102(b) as being anticipated by Kocher et al. (6,289,455), referred to as Kocher.

These rejections are traversed for the reasons stated below.

Drawing Objections

Figure 3 was objected to as including a typographically error "INDENTIFIES". Enclosed is a corrected drawing sheet for figure 3 including "IDENTIFIES". Accordingly, withdrawal of the objection is requested.

Claim Rejections Under 35 USC §112 Second Paragraph

Claims 1-36 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Independent claim 1 was rejected because "the first key", "the second key", and "the insecure device" allegedly lack antecedent basis. Independent claim 1 and its dependent

claims only reference one first key (*i.e.*, a first cryptographic key), and only reference one second key (*i.e.*, a second cryptographic key), and only reference one insecure device (*i.e.*, an insecure decryption device). Accordingly, the Applicants believe "the first key" clearly refers to the claimed first cryptographic key, "the second key" clearly refers to the claimed second cryptographic key, and "the insecure device" clearly refers to the claimed insecure decryption device. Thus claim 1 is believed to be definite. Similar rejections were made for independent claims 11, 17, 19, 26, 28 and 36, and these claims are also believed to be definite.

Independent claim 17 recites "the first cryptographic key" without antecedent basis. Independent claim 17 has been amended to recite "a first cryptographic key".

For at least these reasons withdrawal of the rejections under 112 second paragraph is requested.

Claim Rejections Under 35 U.S.C. §102

The test for determining if a reference anticipates a claim, for purposes of a rejection under 35 U.S.C. § 102, is whether the reference discloses all the elements of the claimed combination, or the mechanical equivalents thereof functioning in substantially the same way to produce substantially the same results. As noted by the Court of Appeals for the Federal Circuit in *Lindemann Maschinenfabrick GmbH v. American Hoist and Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984), in evaluating the sufficiency of an anticipation rejection under 35 U.S.C. § 102, the Court stated:

> Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim.

Therefore, if the cited reference does not disclose each and every element of the claimed invention, then the cited reference fails to anticipate the claimed invention and, thus, the claimed invention is distinguishable over the cited reference.

Claims 1-36 were rejected under 35 U.S.C. §102(b) as being anticipated by Kocher.

According to an embodiment described in the Applicants' specification, a device, such as a media player, that is operable to read a secure token, sends its unique ID, N_j, to a server, for example, to purchase a media file. After the purchase, the server sends a first cryptographic key K_1 to the secure token. The server also uses a secure hash function to generate a second cryptographic key K_2 from the first cryptographic key and the unique ID of the media player as follows: $K_2=H(K_1,N_j)$. The server encrypts the media file with K_2 and sends it to the media player. The secure token gets N_j from the media player and calculates K_2, and sends K_2 to the media player. The media player may then decrypt the media file with K_2 received from the secure token and play the media file. See paragraphs 27-34 and figure 3. The unique ID of the device is a message of the device, such as a serial number. Another type of message unique to the media player and stored in the media player may be used to generate K_2. See paragraph 62. As described above, it should be noted that in these embodiments, a message unique to the media player, such as serial number, is used to generate K_2.

Claim 1 recites,

> creating a second cryptographic key from the first key and a message unique to the insecure device, the second key usable for file decryption by the insecure device.

Kocher fails to teach creating a second key from a first key and a message unique to an insecure device. The rejection alleges this feature is taught in col. 8, lines 17-28 of Kocher. In this passage, Kocher discloses a Key Derivation Message (KDM), which is a message generated by the content provider to allow a CRU to derive a key corresponding to digital content, and the KDM is usually transmitted with the content.

However, Kocher fails to teach that the KDM is unique to an insecure device. Instead, unlike the embodiments of the Applicants' invention where the unique message is initially stored in the insecure device and sent to the server, in Kocher the KDM is generated by the content provider and sent to the playback device 210. Thus, it appears Kocher generates a KDM for each content rather than a KDM unique to the playback device. There is no disclosure in Kocher teaching the KDM is unique to the playback device 210.

Independent claim 11 recites using a hash function to create a second key from the first key and a message unique to the insecure device. Kocher fails to teach the hash function, the message unique to the insecure device, or using a hash function to create a second key from the first key and the message unique to the insecure device.

Independent claim 17 recites a data rights management server receiving a unique identifier from the insecure device. As described above, Kocher fails to teach the content provider receiving a unique identifier for the playback device from the playback device. Instead, the KDM is generated at the content provider and is not received from the playback device. Also, the KDM is not unique to the playback device.

Independent claims 19, 28 and 36 recite accessing a message unique to the insecure device. Independent claim 26 recites sending a message unique to the insecure device. These features are not taught by Kocher.

Many of the features of the dependent claims are not taught by Kocher. Claim 7 recites the secure token conducts a transaction with a peer to sell a file. Claim 8 recites the secure token creates a third key unique the peer and sends the third key to the peer and the insecure device. Kocher fails to teach the smart card is used to sell a file, and fails to teach creating a third key for the peer and sending the third key to both the peer and the playback device. Claim 15, 16, 24 and 25 recite similar features.

For at least these reasons claims 1-28 and 30-36 are believed to be allowable.

RECEIVED
CENTRAL FAX CENTER

OCT 0 3 2007

PATENT

Atty Docket No.: 200207237-1
App. Ser. No.: 10/733,434

Conclusion

In light of the foregoing, withdrawal of the rejections of record and allowance of this application are earnestly solicited.

Should the Examiner believe that a telephone conference with the undersigned would assist in resolving any issues pertaining to the allowability of the above-identified application, please contact the undersigned at the telephone number listed below. Please grant any required extensions of time and charge any fees due in connection with this request to deposit account no. 08-2025.

Respectfully submitted,

Dated: October 3, 2007 By

Ashok K. Mannava
Registration No.: 45,301

MANNAVA & KANG, P.C.
8221 Old Courthouse Road
Suite 104
Vienna, VA 22182
(703) 652-3822
(703) 865-5150 (facsimile)

PAGE 20/20 * RCVD AT 10/3/2007 11:20:26 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-3/18 * DNIS:2738300 * CSID:7038655150 * DURATION (mm-ss):04-36